

Appl. No. 09/397,455

Attorney Docket: 042390.P6764

LISTING OF THE CLAIMS:

This listing of claims replaces all prior versions, and listings, of claims in the application:

- 1 1. (Previously Presented) A method comprising:
 - 2 reading from a software module embedding one of a set of key associated with a trusted
 - 3 source;
 - 4 determining whether a key is traceable to one of the set of keys;
 - 5 determining whether the key is identified in a list of compromised keys; and
 - 6 if the key is not identified as compromised and is traceable to one of the keys in the set,
 - 7 assigning the key a trusted status.
- 1 2. (Original) The method of claim 1 further comprising:
 - 2 verifying the integrity of a document comprising the key and the list of compromised
 - 3 keys.
- 1 3. (Cancelled)
- 1 4. (Original) The method of claim 1 in which determining whether the key is traceable to one of
 - 2 the set of keys further comprises:
 - 3 tracing the key through a certificate chain to one of the keys in the set of keys.
- 1 5. (Original) The method of claim 1 further comprising:
 - 2 associating a document comprising the key and the set of keys with a software module
 - 3 comprising the set of keys using a hash of the software module in the document.

Appl. No. 09/397,455

Attorney Docket: 042390.P6764

1 6. (Original) The method of claim 2 in which the document is a manifest signed by the key.

1 7. (Original) The method of claim 1 in which determining whether the key is identified in the list
2 of compromised keys further comprises:
3 searching the list of compromised keys for the key.

1 8. (Original) A method comprising:
2 producing a document comprising an identification of a software module and a list of
3 compromised keys; and
4 digitally signing the document using a key traceable to one of a set of keys comprised by
5 the software module.

1 9. (Original) The method of claim 8 in which the identification of the software module comprises
2 a hash value of the software module.

1 10. (Original) The method of claim 8 in which the key is traceable to one of the set of keys
2 comprised by the software module by way of a certificate chain.

1 11. (Original) The method of claim 8 further comprising:
2 making the document available on a communication network by which computer systems
3 comprising the software module may read the document.

Appl. No. 09/397,455

Attorney Docket: 042390.P6764

1 12. (Original) The method of claim 8 in which the set of keys is embedded within the software
2 module.

1 13. (Original) A device comprising:
2 a processor;
3 a machine-readable storage medium coupled to the processor by way of a bus, the storage
4 medium storing instructions which, when executed by the processor, cause the device to
5 determine whether a key is traceable to one of a set of keys associated with a trusted source;
6 determine whether the key is identified in a list of compromised keys; and
7 if the key is not identified as compromised and is traceable to one of the keys in the set,
8 assign the key a trusted status.

1 14. (Original) The device of claim 13 in which the instructions, when executed by the device,
2 further cause the device to:
3 verify the integrity of a document comprising the key and the list of keys.

1 15. (Original) The device of claim 13 further comprising a software module comprising the list
2 of keys.

1 16. (Original) The device of claim 13 in which the instructions, when executed by the device,
2 further cause the device to:
3 trace the new key through a certificate chain to one of the keys in the set of keys.

Appl. No. 09/397,455

Attorney Docket: 042390.P6764

1 17. (Original) A device comprising:
2 a processor;
3 a machine-readable storage medium coupled to the processor by way of a bus, the storage
4 medium storing instructions which, when executed by the processor, cause the device to:
5 produce a document comprising an identification of a software module and a list of
6 compromised keys; and
7 digitally sign the document using a key traceable to one of a set of keys comprised by the
8 software module.

1 18. (Original) The device of claim 17 in which the identification of the software module
2 comprises a hash value of the software module.

1 19. (Original) The device of claim 17 in which the key is traceable to one of the set of keys
2 comprised by the software module by way of a certificate chain.

1 20. (Previously Presented) An article comprising a machine-readable medium having stored
2 thereon instructions which, when executed by a processor, result in:
3 reading from a software module embedding one of a set of key associated with a trusted
4 source;
5 determining whether a key is traceable to one of the set of keys;
6 determining whether the key is identified in a list of compromised keys; and
7 if the key is not identified as compromised and is traceable to one of the trusted keys,
8 assigning the key a trusted status.

Appl. No. 09/397,455

Attorney Docket: 042390.P6764

1 21. (Original) The article of claim 20 in which the instructions, when executed by the processor,
2 further result in:
3 verifying the integrity of a document comprising the key and the list of keys.

1 22. (Original) The article of claim 20 further comprising a software module embedding the set of
2 keys associated with the trusted source.

1 23. (Previously Presented) The article of claim 20 in which the sequence of instructions, when
2 executed by the processor, further result in:
3 tracing the key through a certificate chain to one of the keys in the set of keys.

1 24. (Original) An article comprising a machine-readable medium having stored thereon
2 instructions which, when executed by a processor, result in:
3 producing a document comprising an identification of a software module and a list of
4 compromised keys; and
5 digitally signing the document using a key traceable to one of a set of keys comprised by
6 the software module.

1 25. (Original) The article of claim 24 in which the identification of the software module
2 comprises a hash value of the software module.

Appl. No. 09/397,455

Attorney Docket: 042390.P6764

- 1 26. (Original) The article of claim 24 in which the key is traceable by way of a certificate chain
- 2 to one of the set of keys embedded in the software module.